PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-028407
(43)Date of publication of application : 31.01.1995

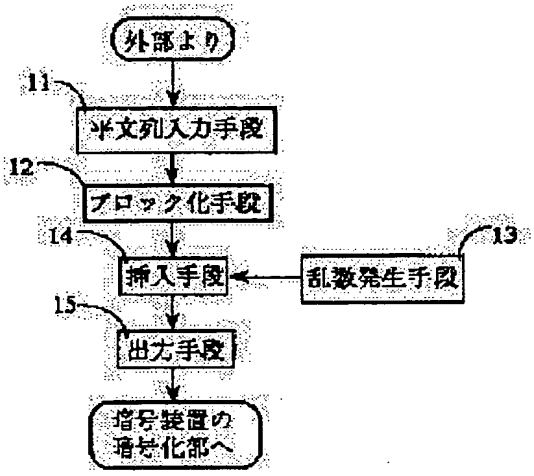
(51)Int.Cl. G09C 1/10
H04L 9/06
H04L 9/14

(21)Application number : 05-174526
(22)Date of filing : 14.07.1993

(71)Applicant : NEC CORP
(72)Inventor : MIYANO HIROSHI
MIYAUCHI HIROSHI

(54) CIPHERING PREPROCESSOR AND DECIPHERING POSTPROCESSOR BY CIPHER

(57)Abstract:
PURPOSE: To provide a ciphering device and a deciphering device which prevent a cipher key from easily being estimated even when a 3rd party knows both a plaintext and a ciphertext by inserting random bits into the plaintext by a cipher system.
CONSTITUTION: The ciphering preprocessor which preprocesses the input of the ciphering device has an input means 11 which inputs an array of plaintexts to be ciphered, a block dividing means 12 which sections the inputted plaintext array by predetermined length into blocks, and a random number generating means 13 which repeatedly generate the random bits. Further, the processor has an inserting means 14 which inserts the random bits generated by the random number generating means 13 at predetermined positions of the respective blocks generated by the block dividing means 12 and an output means 15 which passes the blocks, having the random bits inserted by the inserting means 14, to the ciphering device in order.



LEGAL STATUS

[Date of request for examination]	14.07.1993
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2546504
[Date of registration]	08.08.1996
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平７－２８４０７

(43)公開日　平成７年（１９９５）１月３１日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
G09C 1/10		8837-5L		
H04L 9/06				
9/14				
			H04L 9/02　Z	

審査請求　有　請求項の数2　ＯＬ　（全４頁）

(21)出願番号　特願平５－１７４５２６

(22)出願日　平成５年（１９９３）７月１４日

(71)出願人　０００００４２３７
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　宮野　浩
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　宮内　宏
東京都港区芝五丁目７番１号　日本電気株式会社内

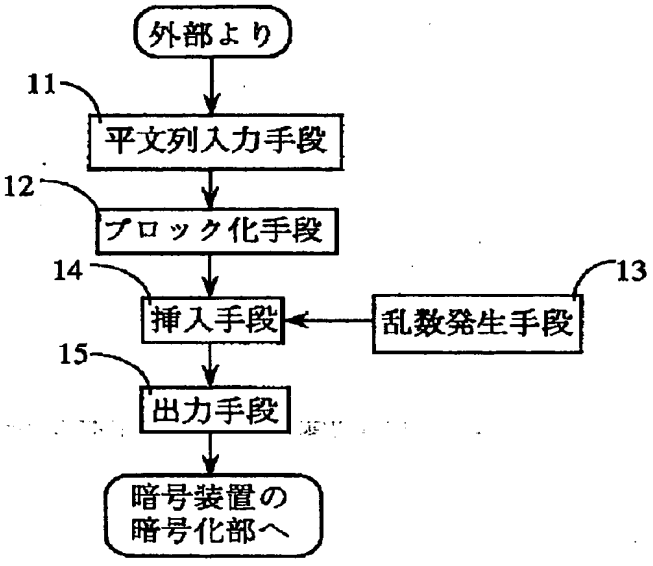
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】暗号における暗号化前処理装置および復号後処理装置

(57)【要約】

【目的】　暗号方式において、平文内にランダムなビットを挿入することによって、たとえ他者に平文と暗号文の両方を知られたとしても暗号鍵を容易に推定されないような暗号化装置および復号装置を提供すること。

【構成】　暗号装置の入力の前処理を行う暗号化前処理装置において、暗号化されるべき平文の列を入力する入力手段１１と、入力された平文列を予め定められた長さ毎に区切ってブロック化するブロック化手段１２と、ランダムなビットを繰り返し発生はする乱数発生手段１３と、上記ブロック化手段によってブロック化されたそれぞれのブロックの予め定められた位置に上記乱数発生手段で発生したランダムなビットを挿入する挿入手段１４と、該挿入手段１４によってランダムなビットを挿入されたブロックを順次暗号装置に受け渡すための出力手段１５を有することを特徴とする。



1

【特許請求の範囲】

【請求項１】　暗号装置の入力の前処理を行う暗号化前処理装置において、暗号化されるべき平文の列を入力する入力手段と、入力された平文列を予め定められた長さ毎に区切ってブロック化するブロック化手段と、ランダムなビットを繰り返し発生する乱数発生手段と、前記ブロック化手段によってブロック化されたそれぞれのブロックの予め定められた位置に前記乱数発生手段で発生したランダムなビットを挿入する挿入手段と、前挿入手段によってランダムなビットを挿入されたブロックを順次暗号装置に受け渡すための出力手段を有することを特徴とする暗号における暗号化前処理装置。

【請求項２】　暗号文を復号する復号装置の出力に対して後処理を施して平文を出力する復号後処理装置において、暗号装置から復号された平文列を受け取るための入力手段と、入力された平文列を予め定められた長さ毎に区切ってブロック化するブロック化手段と、前記ブロック化手段によりブロック化されたそれぞれのブロックから予め定められた位置のビットを除去する冗長ビット除去手段と、前記冗長ビット除去手段によって加工された平文列を最終的な平文として出力する平文列出力手段を有することを特徴とする暗号における復号後処理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、暗号化および復号装置に関するものである。

【０００２】

【従来の技術】ＤＥＳ（昭５１－１０８７０１暗号装置、たとえば「現代暗号理論」池野信一、小山謙二著、社団法人電子情報通信学会１９８６年の第３章に解説）やＲＳＡ（上記「現代暗号理論」第６章に解説）に代表される従来の暗号方式は、平文をある一定長の長さに区切ることによってブロック化し、それぞれのブロックを独立にあるいは順次暗号化することによって平文全体の暗号文を得ることを特徴としている。

【０００３】一般に上記のような従来の暗号系では大きなファイルや通信文を暗号化しようとする場合、平文は多くのブロックに分割される。これらのブロックは通常同一の鍵で暗号化される。このような同一の鍵で暗号化された多数のブロックは、平文が解読者に知れてしまうと、秘密鍵を推定する手がかりとなるおそれがある。

【０００４】

【発明が解決しようとする課題】本発明の目的は、暗号方式において、暗号文と平文の両方が解読者に知れてしまっても秘密鍵を容易に推定することが依然として困難であるようにするための暗号化の前処理装置および復号の後処理装置を提供することである。

【０００５】

【課題を解決するための手段】第１の発明の暗号化前処理装置は、暗号装置の入力の前処理を行う暗号化前処理

2

装置において、暗号化されるべき平文の列を入力する入力手段と、入力された平文列を予め定められた長さ毎に区切ってブロック化するブロック化手段と、ランダムなビットを繰り返し発生する乱数発生手段と、前記ブロック化手段によってブロック化されたそれぞれのブロックの予め定められた位置に前記乱数発生手段で発生したランダムなビットを挿入する挿入手段と、前挿入手段によってランダムなビットを挿入されたブロックを順次暗号装置に受け渡すための出力手段を有することを特徴とする。

【０００６】第２の発明の復号後処理装置は、暗号文を復号する復号装置の出力に対して後処理を施して平文を出力する復号後処理装置において、暗号装置から復号された平文列を受け取るための入力手段と、入力された平文列を予め定められた長さ毎に区切ってブロック化するブロック化手段と、前記ブロック化手段によりブロック化されたそれぞれのブロックから予め定められた位置のビット除去する冗長ビット除去手段と、前着冗長ビット除去手段によって加工された平文列を最終的な平文として出力する平文列出力手段を有することを特徴とする。

【０００７】

【作用】本発明における暗号化の前処理および後処理について述べる。

【０００８】一般に暗号方式は、単に暗号文から平文が推定できないだけではなく、暗号文と平文の組から暗号鍵が容易に推定できないことが要求される。

【０００９】本発明の暗号化前処理装置および復号後処理装置においては、本来の平文に冗長ビットを挿入することにより実際に暗号化装置の入力となる平文を生成する仕組みになっている。挿入されるビット列は暗号化を行う装置と同じ装置内で暗号化処理の直前に生成することが可能なので通常の平文と比較してその内容が第三者に漏れる可能性が著しく小さい。したがって、本来の平文が漏れたとしても実際に暗号化に用いられた平文の全容を知られる可能性はほとんどなく、結果として既知平文攻撃を喫するおそれが小さい。

【００１０】また、挿入するビットはその内容を予め受信者と打ち合わせておく必要がなく、ブロック長と付加するビットの位置だけを打ち合わせておけば十分であり、しかもこれらの情報は秘密にしておく必要もない。したがって、送信者および受信者が管理しなければならない秘密情報が増えることはない。

【００１１】

【実施例】図１に第１の発明の暗号化前処理装置の実施例を、図２に図１の実施例中に用いる乱数発生手段の一構成例を、図３に第２の発明の復号後処理装置の実施例を示した。

【００１２】図１において暗号化前処理装置は、平文列入力手段１１、ブロック化手段１２、乱数発生手段１３、挿入手段１４および出力手段１５とからなる。平文

の列が平文入力手段１１から入力されると、ブロック化手段１２において該平文列を予め定められたビット数毎に区切りブロック化する。挿入手段１４では、乱数発生手段１３で生成されたランダムなビットを各々のブロックの予め定められた位置に挿入する。出力装置１５はその結果得られたビットの列を暗号化装置の入力として暗号化装置に受け渡す。

【００１３】図２は、第１の発明の暗号化前処理装置の一構成要素である乱数発生手段１３の一構成例である。この例では、計算機内のタイムスタンプを暗号鍵、初期定数を平文としてＤＥＳによる暗号化を行い、暗号文を回帰させて繰り返し暗号化を行う。この際、暗号文の先頭の１ビットをランダムなビットとして挿入手段１４に受け渡す。挿入手段１４がランダムなビットを１ビット要求する度に、上記ＤＥＳによる暗号化を行うことにより、乱数発生手段１３としての機能が実現される。

【００１４】図３において復号後処理装置は、入力手段３１、ブロック化手段３２、冗長ビット除去手段３３および平文列出力手段３４とからなる。入力手段３１は、暗号装置の復号装置から復号処理の済んだビット列を受け取りブロック化手段３２に受け渡す。ブロック化手段３２は該ビット列をあらかじめ定められたビット数毎に区切りブロック化し、冗長ビット除去手段３３に受け渡す。冗長ビット除去手段３３は、受け取った核ブロックの予め定められた位置のビットを除去し平文列出力手段３３に受け渡す。平文列出力手段３４は受け取ったビット列を外部に出力する。

【００１５】上記実施例における各ビット列の構造の例を図４に示す。図４においてもとの平文列は上記ブロック化手段１２において既にブロック化されたものを表している。このブロック長は、必ずしも暗号化装置固有のブロック長と一致する必要はない。もとの平文列（ｐ１，ｐ２，．．．）は、上記実施例において平文列入力手段１１が外部より受け取る平文列および平文列出力手段３３が外部に出力する平文列であり、暗号装置用の平文は図１の出力手段１５から暗号連鎖装置の暗号化部に

手渡され、かつ暗号連鎖装置の復号部から図３の入力手段３１に手渡されるビット列である。黒く描かれている部分が挿入手段１４で挿入され冗長ビット除去手段３３で除去される冗長ビットに該当する。

【００１６】

【発明の効果】本発明では、暗号化処理されるブロックの予め定められた位置にランダムなビットを冗長な情報として挿入し、この冗長なビットは他とは全く独立に生成しうるので暗号が解読されてしまった場合意外には他に洩れる虞はない。したがって、選択平文攻撃は既知平文攻撃を行い得る解読者に対してもこのビットは未知の情報となり、解読を困難にする。暗号文の正当な受信者にとって、復号の際にこの冗長ビットをあらかじめ知っている必要はなく、共用すべき秘密情報が増大することもない。よって従来の暗号方式の安全性をより高めることができる。

【図面の簡単な説明】

【図１】第１の発明の暗号化前処理装置の一実施例を示すブロック図。

【図２】第１の発明における乱数発生手段の一構成例を示すブロック図。

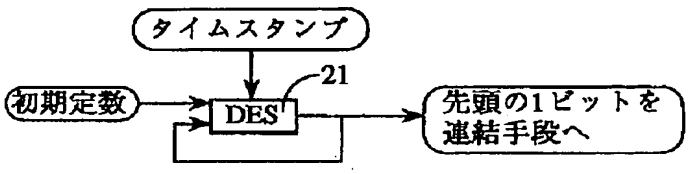
【図３】第２の発明の復号後処理装置の一実施例を示すブロック図。

【図４】本発明において取り扱われるビット列の構造の一例を示す図。

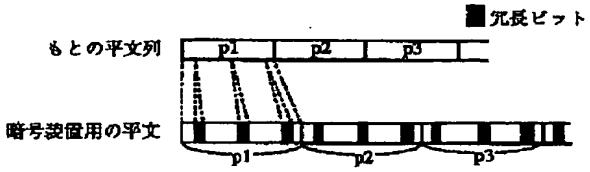
【符号の説明】

１１　平文列入力手段
１２　ブロック化手段
１３　乱数発生手段
１４　挿入手段
１５　出力手段
２１　暗号化装置ＤＥＳ
３１　入力手段
３２　ブロック化手段
３３　冗長ビット除去手段
３４　平文列出力手段

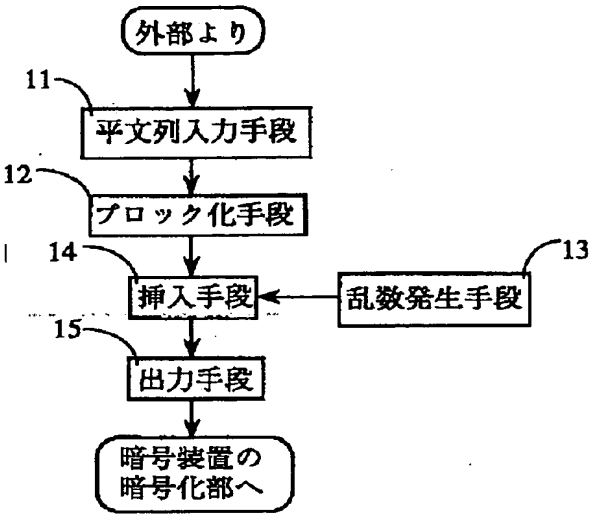
【図２】



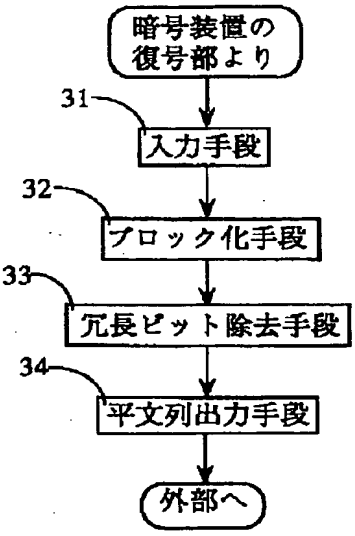
【図４】



【図１】


外部より
11
平文列入力手段
12
ブロック化手段
14
挿入手段
13
乱数発生手段
15
出力手段
暗号装置の
暗号化部へ

【図３】


暗号装置の
復号部より
31
入力手段
32
ブロック化手段
33
冗長ビット除去手段
34
平文列出力手段
外部へ